Managing Departing Employees

Are you prepared?

KPMG

MinterEllison

Navigating the risks associated with departing employees

When an employee leaves your organisation, there is a risk they could take critical confidential information and intellectual property (IP) with them. This has the potential to compromise your organisation's reputation and position in the marketplace. It may also cause a range of adverse direct or indirect impacts. These may include reduction in sales or services, loss of stakeholder confidence (e.g. customers, suppliers, shareholders, etc.), absorption of management's time to deal with the matter, investigation and legal fees and heightened scrutiny or attention from regulators or the media.

In this article, MinterEllison and KPMG provide you with tips and tricks to minimise the risks associated with employee departures and act quickly to protect your organisation should an adverse event occur.

Protecting confidential information and IP now

All employees have an ongoing obligation not to disclose confidential information and IP they obtain during their employment for the benefit of a third party or for their own gain. However, it is *always* best for employers to expressly address employee's obligations in the **employment contract**.

Contractual clauses

You can do this by including carefully drafted and targeted restraint of trade, confidentiality and IP clauses in employment contracts.

Restraint clauses

You will often hear restraints *'aren't worth the paper they're written on'*. Not true! A properly considered and carefully drafted restraint can be a powerful tool.

In determining whether a restraint of trade clause is reasonable, the Courts will have regard to matters including:

(a) the risk that the restraint seeks to protect;

(b) whether the clause goes further than is reasonable to protect against the risk, having regard to the scope of the restraint, the area and the duration;

(c) the seniority of the employee's position;

(d) special features of the business or industry; and

(e) the practical effect of the restraint.

While the Courts have been prepared in some cases to sever an unreasonable provision in a restraint clause, they will stop short of reconstructing the clause to exact a reasonable scope and will not enforce a restraint clause which is too broad.

To maximise the enforceability of a restraint, you should:

(a) avoid using cascading restraint clauses where possible (i.e. listing a series of overlapping alternatives for timeframes, areas and scope); and

(b) tailor the clause to the individual and the role they will play in your organisation.

Confidential information and IP clauses

To maximise enforceability, clauses should be tailored to protect the information accessible to an employee as a result of their role.

You should be aware that a former employee will only be prevented from using confidential information if the information is *genuinely* confidential. Items such as client lists, business forecasts, trade secrets, and sales and marketing plans will generally be considered confidential. General know-how or knowledge acquired by an employee as part of the performance of their duties (e.g. publicly available information about the key players in an industry) will not be considered confidential information capable of protection.

Contractual clauses alone will not always be enough. It is imperative you treat the most confidential information or trade secrets like the 'Holy Grail'. If the janitor or a brand administration clerk in the call centre could access your pricing formulas or key client lists, the Courts will not be quick to protect what you did not protect.

Training, policies and procedures

You should seize any opportunity you can to reinforce confidentiality and IP obligations with employees through:

(a) training on induction as well as regular refresher training during employment; and

(b) clear policies detailing the employee's obligations and your organisation's position on access to, and use of, confidential information and IP.

Ideally, you should keep the conversation about these matters flowing throughout the employment relationship.

Exit Interviews

An exit interview is also an opportunity to remind an employee of their continuing obligations regarding confidentiality, IP, restraints (if any) and to return company property including phones, computers and documents.

Obligations under the Corporations Act

Under the *Corporations Act 2001* (Cth), employees are prevented from using confidential information obtained during the course of their employment with an organisation to gain an advantage for themselves or to cause detriment to the organisation. Employees who breach these obligations can face civil penalties.

Limit access

Employees should only have access to the information required to perform their role. For example, an employee working in your logistics team does not require access to the human resources or payroll files. Likewise, a salesperson doesn't need access to the blueprints for your latest ground breaking widget.

- At a minimum, data stored on your network should be divided into functional areas with access controls limiting access to relevant employees only.
- Consider utilising electronic file access controls options or an electronic document management system (EDMS), as the potential benefits may include the following.
  - access control privileges, which can be granted/restricted based on each position or individual's role.
  - audit logging capabilities, which provides a secure record of the access, modification and deletion of your documents by employees.
  - version control, which allows you to see what user and information changed in a document.
- Implement a security classification system for employees to use on information (eg. emails or documents) as a reminder on the information's private or confidential nature. This may also serve as a flag to the employee as to whom it may be appropriate to disclose this information and what security measures may need to be implemented.

Secure, monitor or remove information exit points

Consider the methods by which information can leave your organisation. Are they all required for business-as-usual (BAU) activities? Are they secure? The following technology solutions may assist.

- Encryption may be used on portable storage devices or emails to protect valuable information in circumstances where it needs to be shared with third-parties. This helps prevent opportunities to 'inadvertently' distribute this information.
- Group policies and certain software can be used to remove write access to storage devices (USBs or portable hard drives) and optical media (CD/DVDs).
- A proxy server or web filter can be used to restrict or monitor information leaving your organisation via internet file sharing sites such as Dropbox, One Drive, etc. or web based personal email services such as Hotmail, Gmail, etc.
- Implement and retain print and security access logs, which can have automatic alerts sent when unusual activity occurs.

Whilst these measures won't guarantee that private or confidential information will not leave your organisation, they certainly reduce the number of ways it can. In the case of monitoring, they may act as a deterrent to any employees considering taking confidential information and provide vital evidence in the event of actual or suspected loss of information.

Some of these options are inexpensive, others less so. Consider the value of your organisation's information and the monetary, legal and reputational ramifications of it falling into the wrong hands when assessing the value proposition of various solutions.

What to do when the horse has bolted

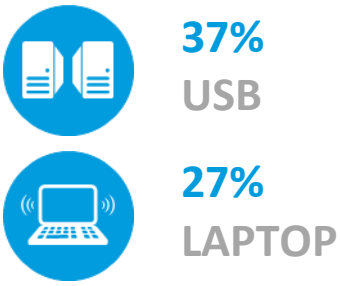
Forensic analysis

An organisation needs to respond quickly to any allegation or concern of information leakage.

This is critical to help:

- **secure** available evidence in a forensically sound manner
- **uphold** evidential integrity for the investigation, and
- **mitigate** distribution of the information and any legal or reputational damage caused by the theft.

Those taking this information are often conscious of the trail of evidence available when web based email or cloud storage sites are used. As a result, they are likely to use physical storage media.



This means from an organisation's perspective, it is crucial to know what actions were carried out on the employee's devices in the lead up to their departure. Whilst organisations often have in place IT policies to restrict or monitor the uploading of information to cloud storage or personal email, a review of the usage of physical media is often not conducted. This is especially relevant for 'high-value individuals', such as the C-suite or those in certain parts of the organisation who have access to sensitive material. This means identifying the source of the theft of information often goes unnoticed.

In an attempt to limit any potential loss or damage by departing employees, most organisations already have in place procedures to recover supplied computing equipment, including mobile telephones and laptops, security passes and conduct an exit interview. Few organisations, however, have the skills or capacity in-house to examine the computing devices used by the former employee.

A forensic examination of these devices and the general activities of the departing employee can paint a picture of actions taken in relation to your organisation's information. Often detailed user activity, including references to data contained on portable storage devices, is able to be retrieved even when the devices are no longer present. This may identify any inappropriate actions taken that led to the data breach, and may include the following:

- Capturing and conducting a targeted review on any emails sent on the company server, and if possible any web based providers. This may include any deleted emails able to be recovered through the use of specialist forensic tools.
- Review of records of USB or portable hard drives connected to the former employee's computer, and any evidence of confidential information that may have been copied to those devices. This analysis can still be highly valuable even if the storage device is long gone. Computers can still retain information for months or even years.
- Inspection, where available, of logs pertaining to documents printed or records accessed by the departing employee.
- Examining calls placed just prior to the employee leaving to check phone numbers against a list of clients, competitors, or other numbers-of-interest.
- Interviews with employees who report to the departing employee, especially personal assistants or employees with similar roles, as they may have been asked to gather information on behalf of the departing employee.

According to research on the theft of data and intellectual property (IP) by McAfee and Intel Security when company information is stolen

43% OF INCIDENTS
the culprit is found to be a malicious insider

60% OF CASES
the target is the information of your customers or employees **not** intellectual property

Demand on former employee

What happens if, despite your best efforts, you have a rogue employee or former employee attempting to use your confidential information or IP for their own benefit or the benefit of a competitor? You have options.

Where your organisation has a reasonable suspicion that a former employee has breached their restraint and/or taken confidential information or IP, you can write to the former employee:

(a) reminding them of their obligations (including those set out in their employment contract);

(b) putting them on notice that the organisation is aware that the employee may be breaching those obligations;

(c) depending on the circumstances of the case –

  (i) requiring the employee to cease their behaviour;

  (ii) requiring the employee to return all documents and information concerning the organisation's business and to delete any electronic records containing the organisation's confidential information/IP;

  (iii) ascertaining from the employee whether they have provided any confidential information to third parties; and;

  (iv) having them sign an undertaking to ensure that any documents are returned and electronic files destroyed.

Court intervention

Where an employee/former employee does not respond or refuses to comply with a demand, you may want to take legal action against the employee. This may involve applying to the Court for:

(a) an interlocutory injunction stopping the employee from engaging in the restrained activities or from using/disclosing confidential information or IP (pending trial);

(b) an account of profits and/or liquated damages if the restraint period has passed and it can be established that the organisation has suffered damage as a result of the breach;

(c) an order for the employee to deliver up and/or destroy documents containing the confidential information/IP.

If you believe writing to the employee and making a demand might cause them to destroy evidence or, worse yet, destroy your organisation's property, you could considering seeking an Anton Pillar Order. This permits a compulsory search of the employee's home and/or their new business premises to gather evidence of a likely breach of the restraint or breach of confidence. These are an expensive, but sometimes very useful tool.

While the risk of departing employees taking and using confidential information and IP can be a daunting one, the risk can be managed through a combination of employment and technology measures. We recommend you be proactive throughout the relationship and take steps to protect your position. Check your contracts, check your policies and, above all, ensure you keep sensitive confidential information under lock and key (probably digitally these days). It's need to know only.

Be proactive throughout the employment relationship and take steps to protect your position.

We are here to help

MinterEllison

Rhian O'Sullivan
Senior Associate

T +61 7 3119 6463
M +61 421 741 587
E rhian.osullivan@minterellison.com

Rhian is a Senior Associate in the Human Resources and Industrial Relations group at MinterEllison.

Rhian has a range of experience in employment law including work health and safety, general protections claims, unfair dismissals, sexual harassment and discrimination claims and general litigation.

She has advised private and public sector clients in industries including mining, energy, construction, education, health and insurance and has assisted in the conduct of litigation in courts and tribunals in State and Federal jurisdictions.

Sarah Walters
Senior Associate

T +61 7 3119 6516
M +61 466 309 004
E sarah.walters@minterellison.com

Sarah is a Senior Associate in the Human Resources and Industrial Relations group at MinterEllison.

Sarah has a particular interest in industrial strategy, general employment litigation and alternative dispute resolution.

Sarah has a broad range of experience in employment and industrial law including providing strategic advice on discrimination, general protections, workplace disputes, rights and obligations of employees, employee terminations (including unfair dismissal), performance management and employee misconduct matters.

KPMG

Stephen Roberts
Associate Director

T +61 7 3233 9734
M +61 429 182 321
E stroberts@kpmg.com.au

Stephen is an Associate Director with KPMG Forensic, a Chartered Accountant, and a licensed Private Investigator.

Stephen's Forensic experience includes assisting organisations to prevent or investigate allegations of fraud, corruption or misconduct.

Investigations Stephen has managed or assisted with cover a range of organisations, including government and corporates, and a variety of allegations or suspicions, from more simple matters to allegations of multi-million dollar fraud. These matters have involved investigations being conducted not only in Queensland, but also throughout Australia and abroad.

Michael Taranwsky
Associate Director

T +61 7 3233 3297
M +61 427 747 782
E mtaranwsky@kpmg.com.au

Michael is an Associate Director with KPMG Forensic, an IACIS Certified Forensic Computer Examiner, and a licensed Private Investigator.

Michael has over five years' experience with KPMG, as a digital forensic analyst. Prior to this Michael was a member of the Queensland Police Force's Electronic Evidence Examination and High Tech Crime Units.

Michael's examinations have covered a range of matters including: allegations of fraud, corruption or misconduct, intellectual property theft / information leaks and security incident response forensics. Michael has managed or assisted with digital forensic investigations covering a range of organisations, including government and corporates throughout Australia and abroad.